Editor: Stephen Ruth • ruth@gmu.edu

A Legislator's Dilemma

Stephen Ruth and Samuel Stone • *George Mason University*

Drafting and passing federal laws aimed at curbing online copyright violations or discouraging hacking into private databases has proven difficult enough, but a greater challenge looms: top cybersecurity officials worry that major infrastructure elements such as financial, electrical, and water systems could be taken down if cybersecurity legislation continues to be deferred.

Imagine this if you can — the US's "chief spy," a four-star general, giving a major talk at a significant technology meeting wearing jeans and a logo T-shirt. It happened at the DefCon July 2012 conference in Las Vegas, a gathering of hackers at which 16,000 attendees received this message: "We need great talent. We don't pay as high as everybody else, but we're fun to be around." The appearance of General Keith Alexander, Director of the US National Security Agency (NSA), at a hacker's convention emphasized the importance of hacking expertise to national security.[1] But it also serves as a reminder of the complex relationships between government IT policy interests and those of society in general. Citizens want to be protected against unlawful intrusion into their personal data and to have a reliable power grid that isn't vulnerable to cyberterrorism. When legislation is proposed to accomplish these goals, however, it encounters a formidable array of pressure groups alleging that Internet freedom is being sacrificed. Here, we describe some of the challenges inherent to passing legislation about such critical issues as hacking, cybersecurity, intellectual property, and censorship.

Growing Hactivism

Is the hacker a hero/provocateur who defends the Internet's openness and freedom or a selfish, devious criminal? Examples abound of both roles. "White hat" hackers serve the public good and practice "ethical hacking," usually testing IT systems' limits to prevent breaches or abuse. But most hacking reports aren't in this category. In July 2012, the Yahoo Voices subdomain (previously, Associated Content) was hacked, and the attackers posted more than 450,000 individual log-in credentials to a public site called the D33D Company. The perpetrators left this message: "We hope that the parties responsible for managing the security of this subdomain will take this as a wake-up call, and not as a threat."[2] Was this a crime? A prank? It depends on your perspective. We could consider the incident a service to consumers because it alerted a wide audience to a problem waiting to happen.

The Yahoo Voices hackers didn't identify themselves, but some of the best-known groups have an identity and a history. Anonymous, for example, was founded almost a decade ago and is a loose collective of global hackers whose major goal is a free and censorship-free Internet. Anonymous began gaining public recognition in 2008 for a campaign against the Church of Scientology when that organization attempted to remove online access to controversial interviews with prominent Scientologist Tom Cruise.[3] Since then, Anonymous has expanded its activities broadly, successfully hacking into major sites through distributed denial-of-service (DDoS) attacks and leaking confidential information. In response to British legislation authorizing surveillance of citizens' Internet activities,[4] Anonymous temporarily disabled several UK government sites via DDoS attacks

 1089-7801/12/$31.00 © 2012 IEEE

in April 2012. Reacting to the US's Stop Online Piracy (SOPA) and Protect Intellectual Property (PIPA) acts, Anonymous launched DDoS attacks on government sites such as the Federal Bureau of Investigation (FBI) and the Department of Justice (DoJ), as well as the proposed bills' advocates in the entertainment industry.[5] In July, Anonymous launched extensive attacks against the Australian government, disabling 10 websites via DDoS attack to protest proposed legislation that would make ISPs archive user information for government review.[6] Additionally, Anonymous has expanded its activities beyond anticensorship, announcing that it's hacked into several energy giants, including Shell, ExxonMobil, and BP Global. The cyberattacks compromised hundreds of corporate accounts, and the group released private email addresses and passwords online. The impetus for the attacks against the energy firms was reportedly their drilling for offshore oil in the Arctic.[7]

Another well-known hacking group, WikiLeaks, founded in 2006, had an open contribution policy similar to Wikipedia, but later switched to its current content policy of registered volunteers obtaining information to ensure greater accuracy. WikiLeaks publishes documents acquired from sources and contributors on multiple servers and domain names, making the information easier to procure and harder to block. Still functioning after its famous disclosure of classified documents about the US's war in Afghanistan, WikiLeaks recently claimed to have leaked several high-profile files on the ongoing violence in Syria taken directly from the Syrian government,[8] as well as US diplomatic cables revealing candid details about the US's relationship with Venezuela and Paraguay.[9]

Hacking has become a common occurrence worldwide, and attacks seem to be increasing in audacity and level of penetration. The hactivism culture has fostered the theft of copyrighted materials such as songs, movies, and books as well as frequent unauthorized compromising of supposedly safe government and commercial sites. Yet the greatest threat hactivism poses is to national infrastructure.

Failure to Legislate Against a Future Crisis

Even though hacking, piracy, and online theft are increasing dramatically, legislatures continue to have trouble agreeing on tough laws to stop illegal hacking and other Internet-based security threats. The possibility of an Armageddon-like power outage or financial crisis, frequently predicted by the US intelligence community, hasn't produced legislative results. For example, the US House of Representatives passed a relatively stringent Cyber Intelligence Sharing and Protection Act (CISPA) in April 2012 after considerable debate, but the Senate modified it substantially. The emerging Senate legislation, the Cybersecurity Act of 2012 (S 2150), was significantly less restrictive than the House version but gained what the House bill lacked — presidential support. President Barack Obama described the administration's cybersecurity goals:

> We need to make it easier for these companies — with reasonable liability protection — to share data and information with government when they're attacked. And we need to make it easier for government, if asked, to help these companies prevent and recover from attacks.[10]

Yet, each Senate revision of the CISPA bill seemed to remove more of its initial strength as various lobbying groups such as the Electronic Frontier Foundation (EFF) sought less restrictive language. A later version of the bill finally gained the EFF's reluctant approval but was much-diminished compared to the original House bill.[11] One main feature was that businesses' compliance with cybersecurity mandates would be voluntary through a self-certification process, which would be overseen by a new National Cybersecurity Council, with membership from public and private sectors, the DoJ, the Department of Commerce, and the intelligence community. Other provisions aimed at safeguarding individuals' privacy and letting them bring lawsuits against the government for violating the law's intent — for example, overzealous surveillance. However, on 3 August, just before Congress left for a month-long recess, the bill was defeated, and no active cybersecurity legislation was pending. Sponsors hope to revive it later in the year, or possibly in 2013.

Failure to Legislate Against Piracy

Although the CISPA legislation might someday see new life in the US House and Senate, another ambitious bill aimed at Internet regulation was crushed soundly, and probably won't return any time soon. Early in 2012, SOPA and its Senate counterpart PIPA seemed to be moving well. SOPA, introduced in fall 2011, aimed to combat the trafficking of copyrighted intellectual property. The bill included strict penalties, such as prohibiting advertisers and payment networks from doing business with sites that violated the law and letting court orders force search engines to block access to offenders, including making it a criminal offense to stream prohibited copyrighted content. At first glance, it seemed likely to pass because it had support from the US's powerful Chamber of Commerce, the Motion Picture Association of America, and the Recording Industry Association of America, and was aimed at so-called "rogue

websites" that allegedly threatened 19 million US jobs (www.mpaa.org/contentprotection/roguewebsites). But a coalition of ISPs and watchdog groups such as the EFF, one-day shutdowns of the English-language content on Wikipedia and Reddit, coordinated service blackouts of thousands of other sites, and numerous petitions — including one Google gathered claiming to have 7 million signatures — brought down SOPA/PIPA, and it was removed from further congressional action. Aside from a few attempts to legislate small segments of the former SOPA law, such as requiring US embassies to shift foreign copyright specialists on their staff from State Department to US Patent and Trademark Office supervision, there appears to be little hope for major antipiracy legislation.

Failure to Approve ACTA

Another online copyright protection/antipiracy measure, initiated long before SOPA/PIPA, was an international trade pact called the Anti-Counterfeiting Trade Agreement. ACTA had many provisions similar to SOPA/PIPA and already had agreement from the US, Mexico, Morocco, and many other nations, but in 2008, WikiLeaks disclosed details of the secret international negotiations. Claims were made that ACTA authorized signatory nations to "peer inside your iPod" at border crossings.[12] This disclosure slowed ACTA's progress considerably, but its long-term fate seemed to hang on a decision this summer in the European Parliament. Even though ACTA is still in force for some nations, such as the US and Japan, it was dealt a major blow in July 2012 when, after experiencing a significant barrage of online criticism claiming that it was an anti-Internet and pro-censorship bill, the 27-member-state European Parliament resoundingly defeated it.[13]

Enforcement without New Legislation

Can criminals still be prosecuted despite these failed legislative acts? Several recent arrests indicate that existing statutes could still work, at least in some cases. With respect to hacking, the FBI has released a statement that perpetrators of DDoS attacks face criminal charges that carry a sentence of up to 10 years in prison (www.fbi.gov/news/pressrel/press-releases/warrants_012711). Recently, the State Department determined that documents published without proper authorization, such as the diplomatic cables leaked by WikiLeaks, are still considered confidential and protected by the Freedom of Information Act.[14] Corporations have also taken a stance against WikiLeaks — both MasterCard and Visa retaliated after falling victim to information it released, imposing a financial blockade that prevented donors from funding WikiLeaks through their respective credit cards. Concurrently, the US and UK governments, along with the EU, have coordinated arrests targeting Anonymous members. One member, known as Sabu, has become an informant for the FBI and helped authorities arrest six Anonymous members in the US and Ireland.[15] Similar arrests of suspected Anonymous members have also occurred in the UK and Spain. The largest single roundup of Anonymous members occured in June 2011 in Turkey, with 32 suspects arrested for DDoS attacks on Turkish government websites.[16]

One of the largest online piracy-related busts involved the website MegaUpload, which is accused of encouraging users worldwide to store pirated movies and music.[17] On 19 January 2012, the DoJ shut down the website, which claimed to have 180 million users, filing charges for criminal copyright infringement, racketeering, and money laundering, with alleged illicit gains of US$175 million and an estimated $500 million in damages. However, at this writing, the trial in New Zealand of Kim Dotcom, the company's president, is anything but clear-cut, with struggles over extradition and other legal disputes continuing.[18]

Contrasting Initiatives: US and Russia

In an attempt to be sure that Internet regulation continues to be as free and open as possible — many of the regulating organizations are on US soil — the US House recently passed a unanimous resolution against any increase in the UN's control of the Internet. Several nations had hoped to use the international telecommunications meetings in December to press for more stringent Internet controls.[19] Said one sponsor of the resolution,

> The American people want to keep the Internet free from government control and prevent Russia, China, and other nations from succeeding in giving the UN unprecedented power over Web content and infrastructure.[20]

On the other end of the spectrum, despite claims of censorship and a one-day protest blackout of Russian-language content on Wikipedia, the Russian Duma passed, by a vote of 441 to 9, a bill aimed at blacklisting more than 400 "harmful Internet sites," effective in November 2012.[21]

So, where does this legislation — or lack thereof — leave governments trying to prevent hacking, hactivism, and online piracy? The various laws already available, plus more voluntary action by major search firms, could help keep piracy challenges at bay in the absence of SOPA/PIPA. Google recently announced

that it would voluntarily reduce the search rankings of sites that receive copyright removal notices (http://tinyurl.com/8puu6u8). But the legislative vacuum on cybersecurity and the failure to pass CISPA might be more worrisome. After CISPA's legislative defeat, the US administration began to draft executive orders that didn't require congressional approval as stopgap cybersecurity measures.

In the meantime, the potential dangers of diminished cybersecurity enforcement continue to escalate. As early as October 2009, the popular US news program *60 Minutes* interviewed retired Admiral Mike McConnell, who had served as leader of the Defense Intelligence Agency and the NSA, and, like General Alexander, was America's "chief spy." Speaking on the possibility of a cyberattack on the computer networks that are responsible for distributing power, water, fuel, transportation, and financial transactions, he said, "If I were an attacker and I wanted to do strategic damage to the United States, I would either take the cold of winter or the heat of summer, I probably would sack electric power on the US East Coast, maybe the West Coast, and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker."[22]

References

1. S. Cowley, "NSA Wants to Hire Hackers," *CNN*, 29 July 2012; http://money.cnn.com/2012/07/27/technology/defcon-nsa/index.htm.
2. S. Musil, "Hackers Post 450K Credentials Pilfered from Yahoo," *CNET*, 11 July 2012; http://tinyurl.com/9obbejh.
3. D. George-Cosh, "Online Group Declares War on Scientology," *Nat'l Post*, 26 Jan. 2008; http://tinyurl.com/9yr2hrm.
4. "Anonymous Claims Responsibility for Taking Down Government Sites," *The Guardian*, 8 Apr. 2012; www.guardian.co.uk/technology/2012/apr/08/anonymous-taking-down-government-websites.
5. R. King, "Anonymous Hacks DOJ, RIAA, MPAA, and Universal Music Websites," *ZD Net*, 19 Jan. 2012; www.zdnet.com/blog/btl/anonymous-hacks-doj-riaa-mpaa-and-universal-music-websites/67590.
6. C. Connelly, "Anonymous Hackers Cripple Australian Government Websites," *Fox News*, 24 July 2012; www.foxnews.com/tech/2012/07/24/anonymous-hackers-cripple-australian-govt-websites/.
7. "Anonymous Hackers Target Energy Majors," *UPI*, 18 July 2012; http://tinyurl.com/8vzsmm8.
8. "Syria File," *WikiLeaks*, 5 July 2012; www.wikileaks.org/syria-files/.
9. N. Kozloff, "Condi and Hillary's 'Tug of War' with Chavez in Paraguay," *WikiLeaks Central*, 17 July 2012; http://wlcentral.org/node/2733.
10. A. Fitzpatrick, "Obama Gives Thumbs-Up to New Cybersecurity Bill," *Mashable*, 20 July 2012; http://mashable.com/2012/07/20/cybersecurity-obama/.
11. R. Reitman and L. Tien, "New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities," *Electronic Frontier Foundation*, 19 July 2012; http://tinyurl.com/84699tw.
12. C. Arthur, "The Right to Peer Inside Your iPod," *The Guardian*, 9 July 2008; www.guardian.co.uk/technology/2008/jul/10/intellectualproperty.law.
13. C. Arthur, "ACTA Down, But Not Out, as Europe Votes Against Controversial Treaty," *The Guardian*, 4 July 2012; www.guardian.co.uk/technology/2012/jul/04/acta-european-parliament-votes-against.
14. W. Oremus, "Judge Rules that Wikileaks Cables Are Still Secret," *Slate*, 24 July 2012; http://tinyurl.com/9a6qd36.
15. C. Long, "Hackers Busted After 1 Becomes FBI Informant," *Seattle Pi*, 10 Mar. 2012; www.seattlepi.com/business/article/Hackers-busted-after-1-becomes-FBI-informant-3390667.php.
16. C. Albanesius, "Turkey Arrests 32 'Anonymous' Members," *PCMag*, 13 June 2011; www.pcmag.com/article2/0,2817,2386803,00.asp.
17. G. Gross, "DOJ Files Additional Charges in MegaUpload Case," *PC World*, 17 Feb. 2012; http://tinyurl.com/8nyfx7j.
18. W.M. Welch, "Defense Seeks to Toss Dotcom MegaUpload Piracy Case," *USA Today*, 29 July 2012; http://tinyurl.com/8dqbheg.
19. S. Ruth, "Is There a Digital Divide? Check the Numbers," *IEEE Internet Computing*, vol. 16, no. 4, 2012, pp. 80–83.
20. J. Smith, "House Unanimously Approves UN Internet Resolution," *Nat'l J.*, 2 Aug. 2012; http://techdailydose.nationaljournal.com/2012/08/house-unanimously-approves-un.php.
21. A. Kilyakov, "Russia Passed Internet Blacklist Bill," *Russia Beyond the Headlines*, 12 July 2012; http://rbth.ru/articles/2012/07/12/russias_authorities_adopted_internet_blacklist_bill_16301.html.
22. "Cyber War: Sabotaging the System," *60 Minutes*, 10 June 2010; www.cbsnews.com/stories/2010/06/10/60minutes/main6568387.shtml.

Stephen Ruth is a professor of public policy at George Mason University. He manages a grant-supported IT research center, the International Center for Applied Studies in Information Technology (ICASIT), which studies contemporary technology deployment issues — most recently, massive open online courses and e-learning telework — and green IT comparisons between the public and private sectors. Contact him at ruth@gmu.edu.

Samuel Stone is a graduate student of global affairs with a specialization in media and information technology at George Mason University. His studies and volunteer work include analysis of social media's impact on culture, the effectiveness and different strategies of viral marketing, and technology-based advancements within public policy. Contact him at sstone4@gmu.edu.